

Форма № ДН-7.02.1

Державний вищий навчальний заклад

«Донецький національний технічний університет»

Кафедра Прикладної математики та інформатики



РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОНД 1.2.13 Безпека програм та даних

(шифр і назва навчальної дисципліни)

Рівень освіти: перший (бакалаврський)

Спеціальність (ості) 121 Інженерія програмного забезпечення

(шифр і назва спеціальності (тей))

Освітня програма 121 Інженерія програмного забезпечення

(назва освітньої програми, для обов'язкових дисциплін)

Мова навчання: українська

Покровськ – 2020

Робоча програма навчальної дисципліни Безпека програм та даних

для здобувачів вищої освіти за спеціальністю 121 Інженерія програмного забезпечення

«1» жовтня 2020 року. – 7 с.

Розробник:

Маслова Н.О., к.т.н., доц., доц. каф. ПМІ

Робоча програма затверджена на засіданні кафедри прикладної математики і інформатики

(назва кафедри)

Протокол № 11 від «1» жовтня 2020р.

Завідувач кафедрою ПМІ

(Дмитрієва О.А.)
(прізвище та ініціали)

«1» жовтня 2020р

Схвалено науково-методичною комісією з галузі знань 12 Інформаційні технології

(шифр, назва)

Протокол № 6 від «7» жовтня 2020р.

«7» жовтня 2020р. Голова

(підпис)

(Башков Є.О.)
(прізвище та ініціали)

1. Загальна інформація

Форма навчання	Денна	Заочна
Статус	ОНД- – Обов'язкова навчальна дисципліна	
Обсяг в кредитах ЄКТС	7	7
Обсяг в годинах за навчальним планом, разом:	210	210
в тому числі:		
лекцій:	48	8
практичні заняття:	32	4
лабораторні заняття:		
семінари:		
самостійна робота:	130	198
Форма підсумкового контролю	<u>Екзамен</u>	
Дисципліну викладають	Викладач І (Маслова Н.О., https://donntu.edu.ua/knt/pmi_nataliia.maslova@donntu.edu.ua)	

Передумови для вивчення дисципліни: перелік дисциплін, які мають бути вивчені раніше: Основи інформаційної безпеки, Архітектура та проектування програмного забезпечення, Теорія синтаксичного аналізу та компіляції, Конструювання програмного забезпечення.

2. Мета вивчення навчальної дисципліни

Метою викладання дисципліни є формування у студентів здібностей до захисту програм і даних, опанування поняттями та базовими стандартами в галузі інформаційної безпеки.

Компетентності:

- Здатність ідентифікувати, класифікувати та формулювати вимоги до програмного забезпечення (K13).
- Здатність брати участь у проектуванні програмного забезпечення, включаючи проведення моделювання (формальний опис) його структури, поведінки та процесів функціонування (K14)
- Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки) (K18).
- Володіння знаннями про інформаційні моделі даних, здатність створювати програмне забезпечення для зберігання, видобування та опрацювання даних (K19).
- Здатність здійснювати процес інтеграції системи, застосовувати стандарти і процедури управління змінами для підтримки цілісності загальної функціональності і надійності програмного забезпечення (K24)
- Здатність обґрунтовано обирати та освоювати інструментарій з розробки та супроводження програмного забезпечення (K25)
- Здатність до алгоритмічного та логічного мислення (K26)
- ФК3 Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах

- ФК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
- ФК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
- ФК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

Програмні результати навчання:

- Знати і застосовувати методи розробки алгоритмів, конструювання програмного забезпечення та структур даних і знань (ПР13)
- Застосовувати на практиці інструментальні програмні засоби доменного аналізу, проектування, тестування, візуалізації, вимірювань та документування програмного забезпечення (ПР14);
- Знати та вміти застосовувати методи верифікації та валідації програмного забезпечення (ПР19);
- Вміти застосовувати методи компонентної розробки програмного забезпечення (ПР17);
- Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних (ПР18);
- Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем (ПР21);
- ПРН14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень
- ПРН20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;
- ПРН26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;
- ПРН29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;
- ПРН47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації
- ПРН50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);
- ПРН53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

3. Очікувані результати навчання

Очікуваними результатами навчання є наявність у студентів навичок з аналізу та захисту програм та даних, надання оцінки результативності й якості прийнятих рішень. В процесі виконання завдань застосовується спеціальне програмне забезпечення, методики й прийоми захисту й аналізу.

В цілому результатами вивчення даної дисципліни є навички з рішення задач захисту інформації від руйнуючих програмних впливів й кодів в інформаційно-телекомунікаційних системах, захист потоків даних, інформації з використанням сучасних методів та засобів криптографії, забезпечення безперервного функціонування програмних та програмно-апаратних комплексів

4. Засоби діагностики результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання можуть бути:

- екзамени;
- розрахункові та розрахунково-графічні роботи;
- презентації результатів виконаних завдань та досліджень;
- виступи на наукових заходах.

5. Критерії оцінювання результатів навчання

Критерії оцінювання мають формулювати порядок оцінювання під час поточного контролю (за результатами практичних, лабораторних, семінарських занять та виконання індивідуальних або групових завдань) та підсумкового контролю.

Поточний контроль							Поточний контроль	Іспит	Максим. сума балів
ПР1	ПР2	ПР3	ПР4	ПР5	ПР6	Інд.РР			
5	5	5	5	5	5	10	40	60	100

Примітка: ПР1, ПР2 і т.д. практичні роботи;
СЗ1, СЗ2 і т.д. семінарські заняття;
ЛР1, ЛР2 і т.д. лабораторні роботи.

Розподіл балів при виконанні практичних робіт для заочної форми навчання

		Поточний контроль	Іспит	Максим. бал
Практ. Роб.1	Практ. Роб.2			
20	20	40	60	100

Схема оцінювання з урахуванням вимог Положення про організацію освітнього процесу. Результати підсумкового контролю оцінюються за 100-бальною шкалою та чотирибальною («відмінно», «добре», «задовільно», «незадовільно»).

Відповідність між шкалами встановлюється наступним чином:

Оцінка	
За 100-бальною шкалою	Для екзамену, курсового проекту(роботи), практики, диференційованого заліку, кваліфікаційного екзамену, випускної кваліфікаційної (дипломної) роботи (проекту)
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

6. Програма навчальної дисципліни

6.1. Основні теми дисципліни

Тема 1. Стратегії та методи забезпечення безпеки програм та даних

Тема 2. Основні поняття інформаційної безпеки

Тема 3. Стандарти інформаційної безпеки

Тема 4. Міжнародні стандарти інформаційної безпеки

Тема 5. Помаранчева книга

Тема 6. Основні поняття криптографії

Тема 7. Симетричні криптосистеми

Тема 8. Асиметричні криптосистеми

Тема 9. Системи захисту інформації та їх функції

Тема 10. Загрози, вразливості та ризики програмного забезпечення

Тема 11. Аналіз ризиків програмного забезпечення, управління ризиками

Тема 12. Програмні Закладки

Тема 13. Принципи захисту програм від НСД

Тема 14. Метод експериментів в захисті програм та даних

Тема 15. Статичний аналіз даних в захисті програмних реалізацій

Тема 16. Динамічний аналіз даних в захисті програмних реалізацій

Тема 16. Захист від дизасемблювання

Тема 17. Захист програм шляхом обфускації

Тема 18. Способи реалізації ускладнення логіки

Тема 19. Додаткові методи боротьби з автоматичними

Тема 20. Захист від несанкціонованого налагоджування

Тема 21. Використання хуків у WINOWS

Тема 22. Сучасні технології дампу і захисту від нього

6.2. Теми практичних (семінарських) занять

№ з/п	Назва теми	Кількість годин	
		Д.ф.н.	З.ф.н.
1	Практична робота 1. Законодавча база з ІБ	4	
2	Практична робота 2. Нех-редактори	6	
3	Практична робота 3. Принципи шифр в криптосистем (RSA)	4	
4	Практична робота 4. Захист програмних реалізацій. Метод експериментів. Архіватори	6	2
5	Практична робота 5. Захист програмних реалізацій. Синтаксичний метод	6	2
6	Практична робота 6. Захист програмних реалізацій. Динамічний метод	6	
...	Усього годин	32	4

6.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		Д.ф.н.	З.ф.н.
1	Проведення практичних занять не передбачено		
...	Усього годин		

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		Д.ф.н.	З.ф.н.
1	Тема 1. Загальні відомості з теорії інформації.	10	14
2	Тема 2. Помаранчева книга – перший стандарт ІБ	10	16
3	Тема 3. Міжнар. співробітництво з каталогізації погроз	10	16
4	Теми 4. Правила створення ПІБ.	10	16
5	Тема 5. Хронологія розробки криптографічних алгоритмів	10	16
6	Тема 6. Застосування Microsoft Visual Studio в захисті програм та даних. Метод Step-Trace в захисті програм та даних	10	15
7	Тема 7. Оцінка складності побудови внутрішньої (вбудованої) або доданої СЗІ	11	16
8	Тема 8 Приклади застосування VPN та VNP каналів.	10	16
9	Тема 9. Оцінювання вартості вбудованої/доданої СЗІ	10	16
10	Тема 10. СВА та СВВ – сучасний підхід до класифікації	10	16
11	Тема 11. Спеціальні засоби захисту ОС 4-го рівня	10	16
12	Тема 12. Сучасні методи антивірусного захисту: застосування хмар	10	16
	Примітка: Індивідуальна розрахункова робота	9	9
...	Усього годин	130	198

6.5. Індивідуальні та/або групові завдання

У рамках курсу для студентів денної та заочної форми навчання передбачено виконання індивідуальної розрахункової роботи на тему: «Дослідження програмних реалізацій, захист програм від аналізу».

В процесі виконання роботи студенти досліджують програмні реалізації з застосуванням методів аналізу, інформації щодо функціонування програм, проводять експертизу програмних реалізацій, їх відповідності задокументованим описам, виявляють вразливості програмного забезпечення та блоки можливо вбудованого шкідливого коду.

7. Література

7.1. Основна

- Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2016. – 544с
- Гломоздра, Дмитро Комп'ютерна вірусологія : навч. посіб. / Дмитро Гломоздра . – Київ : Видавничо-поліграфічний центр НаУКМА, 2012. – 114 с.
- Гришук Р.В., Даник Ю.Г. Основы кибернетической безопасности. За заг.ред.Ю.Г.Даника. Житомир: ЖНАЕУ, 2016. 636с.
- Домашев А.В. Программирование алгоритмов защиты информации : Учебное пособие / Алексей Домашев, Михаил Грунтович, Владимир Попов – М.: Нолидж, 2012. – 416 с.
- Дудатьев А.В. Захист програмного забезпечення. Ч.1 : навчальний посібник / Андрій Дудатьев, Валентина Каплун, Василь Семеренко – Вінниця: ВНТУ, 2005. – 140 с.
- Інформаційна безпека За заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого/ Навчальний посібник / Ю. Я. Бобала, І. В. Горбатий, М. Д. Кіселичник,

А. П. Бондарев, С. С. Войтусік, А. Я. Горпенюк, О. А. Немкова, І. М. Журавель, Б. М. Березюк, С. І. Яковенко, В. І. Отенко, І. Я. Тишик. Львів : Видавництво Львівської політехніки, 2019. 580 с.

- Казарин О.В. Теория и практика защиты программ / Олег Казарин – М.: МГУЛ, 2004. – 450 с.-
- Каплун В.А. Захист програмного забезпечення. Частина 2 : навчальний посібник / В.А.Каплун, О.В.Дмитришин, Ю. В. Баришев – Вінниця : ВНТУ, 2014. – 105с.
- Касперски К. Компьютерные вирусы изнутри и снаружи / Крис Касперски – СПб.: Питер, 2006. – 527 с. –
- Касперски К. Техника и философия хакерских атак / Крис Касперски – М.: Солон-Р, 2006. – 272 с.
- Проскурин В.Г. Защита программ и данных: учеб.пособие для студ.учреждений высш.проф.образования /В.Г.Проскурин. – М.: Издательский центр «Академия», 2012. – 208с.
- Румянцев П.В. Исследование программ Win32: до дизассемблера и отладчика – 2-е изд. доп. / Павел Румянцев – М.: Горячая линия- Телеком, 2014. – 367 с.
- Сенів М. М., Яковина В. С. Безпека програм та даних. Навчальний посібник. Львів : Видавництво Львівської політехніки, 2015. 256 с.
- Соколов А. Защита от компьютерного терроризма : [Справочное пособие] / Алексей Соколов, Ольга Степанюк – БХВ-Петербург: Арлит, 2002. – 496 с
- Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства/ Шаньгин В.Ф. – М.: ДМК Пресс, 2008. – 544 с.
- Методичні вказівки до виконання лабораторних робіт з дисципліни «Безпека програм та даних» для студентів спеціальностей 121 Інженерія програмного забезпечення, 122 Комп'ютерні науки та інформаційні технології, 123 Комп'ютерна інженерія [Електронний ресурс] / уклад. Н.О.Маслова, Т.В.Скрипник. – Покровськ: ДонНТУ, 2017. – 60 с.

7.2 Допоміжна

- Крутое СВ. Защита в операционных системах / С.В.Крутов, И.В.Мащевич, В.Г.Проскурин. — М. : Радио и связь, 2000.
- Мазаник С. Безопасность компьютера: защита от сбоев, вирусов и неисправностей / С.Мазаник . – М.: Эксмо, 2014. – 256с.
- Нужный, В. Використання технологій захисту даних THALES // Енергетика та електрифікація. 2020. № 5. — С. 17-20.
- Шеннон К. Теория связи в секретных системах. Работы по теории информации и кибернетике. – М.: ИЛ, 1963.
- Denning D. Cryptography and data security. Addison- WesleyPublishing Company. 1982. – 400 p.
- Russel D., G.T.Gangemi Sr. Computer Security Basics. – O'Reilli &Associates, Inc., 1991. – 448 p.
- Jackson K., Hruska J. (Ed.) Computer Security Reference Book.Butterworth-Heinemann Ltd., 2016. – 932 p.
- Щербаков А. Построение программных средств защиты от копирования: Практ. рекомендации. — М.: Эдэль, 2019. – 80с

7.3 Методична

- Методичні вказівки до виконання лабораторних робіт з дисципліни «Безпека програм та даних» для студентів спеціальностей 121 Інженерія програмного забезпечення, 122 Комп'ютерні науки та інформаційні технології, 123 Комп'ютерна інженерія [Електронний ресурс] / уклад. Н.О.Маслова, Т.В.Скрипник. – Покровськ: ДонНТУ, 2017. – 60 с
код НТБ ДонНТУ: М124, режим доступу
http://89.185.3.253:9080/list.php?reallist=2&IDlist=Q_1&s_year=up&_id=1601281094746

2. Методичні вказівки до виконання розрахункових робіт з дисципліни «Безпека програм та даних» [Електронний ресурс] : для студентів спеціальностей 121 Інженерія програмного забезпечення, 122 Комп'ютерні науки та інформаційні технології, 123 Комп'ютерна інженерія, 125 Кібербезпека усіх форм навчання / укладач Н.О. Маслова . — Покровськ, 2020 . — 43 с

код НТБ ДонНТУ: М740, режим доступу

http://89.185.3.253:9080/list.php?reallist=2&IDlist=Q_1&s_year=up&_id=1601281094746

8. Інформаційні ресурси

1. В.Б.Белов Основы информационной безопасности // Белов В.Б., Лось В.П. и др., [електронний ресурс], режим доступу <http://www.alleng.ru/d/comp/comp51.htm>
2. Список нормативних документів щодо інформаційної безпеки в Україні // [електронний ресурс], режим доступу [http://uk.wikipedia.org/wiki/Список нормативних документів щодо інформаційної безпеки в Україні](http://uk.wikipedia.org/wiki/Список_нормативних_документів_щодо_інформаційної_безпеки_в_Україні)
3. Безпека програм та даних. Бібліотека ім. Л.Каніщенка Західноукраїнського національного університету, [електронний ресурс], режим доступу - <http://library.tncu.edu.ua/index.php/uk/nmkd/2449-2013-11-11-14-00-08/>
4. Конспект лекцій з дисципліни «Безпека програм і даних. Репозитарій ТНТУ ім. І. Пулюя, [електронний ресурс], режим доступу <http://elartu.tntu.edu.ua/handle/lib/24766?locale=en>
5. Конспект лекцій до дисципліни Безпека програм та даних Луганський національний університет імені Тараса Шевченка, [електронний ресурс], режим доступу <https://studfile.net/preview/5080333/>
6. Мухін В.С. Безпека програм та даних, [електронний ресурс], режим доступу. https://kpi-fict-ip32.github.io/Blog/s07/data_security.html#id56

